Acta Mathematica et Informatica Universitatis Ostraviensis

Cornelius Greither

Galois-Cohen-Lenstra heuristics

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 8 (2000), No. 1, 33--43

Persistent URL: http://dml.cz/dmlcz/120557

Acta Mathematica et Informatica Universitatis Ostraviensis 8 (2000) 33–43

Galois-Cohen-Lenstra heuristics

Cornelius Greither

Abstract: We introduce a new version of the so-called Cohen-Lenstra heuristics concerning predictions how certain class groups are distributed, according to the size of their automorphism groups. Our new ingredient is an action of a Galois group. Some important theoretical results generalize neatly to this equivariant setting. The numerical material which we present is not very ample, due to complexity problems, but it seems to confirm the equivariant heuristics.

Key Words: Class groups, automorphism groups, heuristics, integral representations, modules over group rings

Mathematics Subject Classification: 11R29, 11R33, 20C05

1. Introduction

According to a beautiful idea of H. Cohen and H. Lenstra, the p-part $C_K\{p\}$ of the class group C_K should obey a certain probability distribution as K runs through all imaginary quadratic fields, and this distribution should be given by

$$\mathrm{P}\big(C_K\{p\} \cong G\big) \;=\; c \cdot \mathsf{aut}^{-1}(G).$$

Here G is an arbitrary finite abelian p-group, p a prime number distinct from 2, c is a suitable proportionality factor, and the notation $\mathsf{aut}^{-1}(G)$ is shorthand for $|\mathsf{Aut}(G)|^{-1}$. The idea is thus simply that the larger the automorphism group of G is, the more unlikely it becomes for G to occur as $C_K\{p\}$. Obviously, if the prediction is sound, then the following sum (with G running through all finite abelian p-groups up to isomorphism)

$$S = \sum_G \mathsf{aut}^{-1}(G)$$

must converge, and we must take $c = S^{-1}$.

Indeed, it is a *theorem* of Cohen and Lenstra [2] and Hall [5] that on setting $q = p^{-1}$ one has

$$S = \prod_{i=1}^{\infty}(1-q^i)^{-1} = (q)_\infty^{-1}$$

(the second equality being a definition). Recent work [4] of the author on class groups as Galois modules suggested that it might be interesting to look at $C_K^-\{p\}$ as a $\mathbb{Z}_p[\Delta]$-module where now K is an imaginary abelian field over $\mathbb{Q}$ such that the p-part of $\mathrm{Gal}(K/\mathbb{Q})$ is the p-group Δ. The first obvious question is the following. If we let $\mathbb{Z}_p[\Delta]$-Modf denote the category of finite $\mathbb{Z}_p[\Delta]$-modules, does the sum

$$S'(\mathbb{Z}_p[\Delta]) = \sum_{M \in \mathbb{Z}_p\Delta\text{-Modf}} \mathsf{aut}_{\mathbb{Z}_p\Delta}^{-1}(M)$$

converge? Of course, the sum runs over isomorphism classes of modules M, and $\mathsf{aut}_{\mathbb{Z}_p\Delta}^{-1}(M) = |\mathsf{Aut}_{\mathbb{Z}_p\Delta}(M)|^{-1}$.

We don't have a complete answer, but if Δ is a noncyclic p-group, then the sum diverges, see Section 4. From a certain point of view, this is not yet the right question. In [4] we make very serious use of the fact that under suitable conditions the module $C_K^-\{p\}$ has projective dimension at most 1 over $\mathbb{Z}_p[\Delta]$, so the sum $S'(\mathbb{Z}_p[\Delta])$ contains far too many terms. Let $\mathbb{Z}_p[\Delta]$-Modctf stand for the category of finite $\mathbb{Z}_p[\Delta]$-modules of projective dimension at most 1. (The letters "ct" stand for "cohomologically trivial", and indeed a module over a group ring $\mathbb{Z}_p[\Delta]$ is cohomologically trivial iff its projective dimension is at most 1.)

The next question is therefore: Does the sum

$$S(\mathbb{Z}_p[\Delta]) = \sum_{M \in \mathbb{Z}_p\Delta\text{-Modctf}} \mathsf{aut}^{-1}(M)$$

converge, and if it does, what is its value?

The starting point of this paper is the following result, which was proved in a very complicated manner by the author in 1998 for cyclic p-groups; shortly afterwards, H. Lenstra and B. de Smit [6] found a simple and beautiful proof which actually works for all finite p-groups as well; for simplicity, let us stick to abelian groups.

Theorem 1.1. *For every abelian p-group Δ we have*

$$S(\mathbb{Z}_p[\Delta]) = S.$$

This certainly enhances the importance of the constant S yet another time. (For another context where S appears, see the paper [W] of Washington.)

Actually a more general theorem was proved, both by the author and by Lenstra and de Smit: Let I_Δ denote the augmentation ideal of $\mathbb{Z}_p[\Delta]$, and $M_\Delta = M/I_\Delta M$ the module of coinvariants attached to a $\mathbb{Z}_p[\Delta]$-module M. Then we have:

Theorem 1.2. *If Δ is a finite p-group, supposed abelian for simplicity, then for every finite abelian p-group G there is an equality*

$$S(\mathbb{Z}_p[\Delta]; G) := \sum_{M_\Delta \cong G} \mathsf{aut}^{-1}(M) = \mathsf{aut}^{-1}(G),$$

where M runs through all isomorphism classes of modules in $\mathbb{Z}_p[\Delta]$-Modctf such that M_Δ is isomorphic to G; we recall that $\mathsf{aut}(M)$ refers to automorphisms over $\mathbb{Z}_p[\Delta]$.

Of course, Theorem 1.1 follows from Theorem 1.2 just by summing over all G and applying the Cohen-Lenstra sum formula. In Section 2, we will present the complete proof of Theorem 1.2. My sincere thanks are due to Hendrik Lenstra and Bart de Smit for their permission to include their proof in this note.

The "application" to abelian number fields is now the following. We fix the odd prime p and consider a family of fields K_r, where r is a prime $\equiv 3$ modulo 4 and $\equiv 1$ modulo p; K_r is the unique abelian extension of $\mathbb{Q}$ of degree $2p$ and conductor r. Then K_r is imaginary, and Schoof has shown that the $\mathbb{Z}_p[\Delta]$-module $C^-{}_{K_r}\{p\}$ is indeed cohomologically trivial, where $\Delta \times \{1, j\} = \mathsf{Gal}(K_r/\mathbb{Q})$. (Cf. [4].) The Equivariant Cohen-Lenstra Heuristic would then be:

For any given finite cohomologically trivial $\mathbb{Z}_p[\Delta]$-module M, $P(C^-{}_{K_r}\{p\} \cong M)$ is proportional to $\mathsf{aut}^{-1}_{\mathbb{Z}_p\Delta}(M)$, and hence by Theorem 1.1:

$$P(C^-{}_{K_r}\{p\} \cong M) = S^{-1} \cdot \mathsf{aut}^{-1}_{\mathbb{Z}_p\Delta}(M).$$

There is some numerical evidence for this in case $p = 3$, perhaps somewhat meager; this is discussed in Section 3 below. The reader is advised that the material of that section in particular concerns work in progress and should be considered as tentative. On the other hand, there is a pretty bit of theoretical evidence available, due to Theorem 1.2 and the following observation: K_r contains the imaginary quadratic subfield $\mathbb{Q}(\sqrt{-r})$, and we have a canonical isomorphism afforded by the norm from K_r to $\mathbb{Q}(\sqrt{-r})$:

$$C_{\mathbb{Q}(\sqrt{-r})}\{p\} \cong C^-{}_{K_r}\{p\}_\Delta.$$

Thus the Equivariant C-L Heuristic would imply, by Theorem 1.2, the Standard C-L Heuristic for the imaginary quadratic fields $\mathbb{Q}(\sqrt{-r})$; of course we pretend here that the latter should hold not only for the totality of all imaginary fields but also for the family $\mathbb{Q}(\sqrt{-r})$, which is perhaps a bit rash, but the thing one would expect to happen.

For the case of not necessarily cohomologically trivial modules over $\mathbb{Z}_p[\Delta]$, in which the number-theoretical relevance is not so clear, the question remains whether the Cohen-Lenstra sum $S'(\mathbb{Z}_p[\Delta])$ can be calculated. We conjecture:

If Δ is cyclic of order p^k, then $S'(\mathbb{Z}_p[\Delta]) = S^{k+1}$.

For $k = 0$, this conjecture is nothing new of course; our final result is

Theorem 1.3. *The conjecture is true for $k = 1$.*

The proof is fairly complicated and not very enlightening; it consists in suitably sharpening the technique of proof of 1.2. We do not include it here.

One last thing should be mentioned. In the paper [3], a general situation is discussed, where the class groups are acted on by possibly *non-abelian* groups. However when it comes to modules, it is always arranged that a *maximal order* of the group ring acts on the class group. We on the other hand stick to *abelian* Galois groups, but our main point is that we are particularly interested in modules over *non-maximal orders*, to wit, over the p-adic group ring itself.

Conventions: Without exception, all rings in this paper will be supposed noetherian and unitary, and all modules will be supposed to be finitely generated. This will not be mentioned again.

2. Lenstra's and de Smit's proof of Theorem 1.2

Let Δ be any finite p-group; if the reader prefers, he or she may assume Δ abelian, since this amply suffices for our purpose. Let R be the group ring $\mathbb{Z}_p[\Delta]$. This is a local ring; its radical (i.e., its only maximal ideal) is generated by p and I, the augmentation ideal. Note that $R/I \cong \mathbb{Z}_p$.

We fix a natural number n. Let $F = \mathbb{Z}_p^n$ and $E = R^n$. There is an obvious surjection $\alpha : E \to F$ which identifies $E_\Delta = E/IE$ with F; the kernel of α is IE where I denotes the augmentation ideal of R. The letters L and N will always have a fixed meaning: L is a $\mathbb{Z}_p$-submodule of finite index in F (automatically free), and N is a free R-submodule of finite index in E. We shall always suppose that L is in the radical of F and N in the radical of E, and that $\alpha(N) = L$. As N varies, the quotient $M = E/N$ will vary over all finite R-modules of projective dimension ≤ 1 which require exactly n generators. (Note that if $\mathrm{pd}(M) \leq 1$, the kernel in a projective resolution $0 \to K \to E = R^n \to M \to 0$ has to be free.) The module $M_\Delta = M/IM$ will then be given by $E/(IE + N) = F/\alpha(N) = F/L$, using the convention $\alpha(N) = L$.

For each $L \subset F$ of finite index we let $Y(L) = \{N \subset E : N$ is R-free and of finite index in E, $\alpha(N) = L\}$. We then have

Lemma 2.1. *(a) For every $N \in Y(L)$ the map $\beta : N_\Delta \to L$ induced by α is an isomorphism.*

(b) If $x_1, \ldots, x_n$ is a $\mathbb{Z}_p$-basis of L, then the elements N of $Y(L)$ are exactly the modules $\langle y_1, \ldots, y_n \rangle_R$, where the y_i are R-independent, and $\alpha(y_i) = x_i$ for $i = 1, \ldots, n$.

Proof: (a) Certainly β is onto. Both N_Δ and L are $\mathbb{Z}_p$-free of rank n, so β must be an isomorphism.

(b) If $N \in Y(L)$ and if we pick an R-basis $z_1, \ldots, z_n$ of N, then $\alpha(z_1), \ldots, \alpha(z_n)$ is a $\mathbb{Z}_p$-basis of L; thus it is obtained from $x_1, \ldots, x_n$ via multiplication by a matrix $B \in GL(n, \mathbb{Z}_p)$. The map $GL(n, R) \to GL(n, \mathbb{Z}_p)$ is onto, for instance because the epimorphism $R \to \mathbb{Z}_p$ admits an obvious section, the canonical embedding $\mathbb{Z}_p \to R$. Thus we may lift B to some $C \in GL(n, R)$; if we transform the basis (z_i) with C^{-1}, we obtain a basis (y_i) which maps to the basis (x_i). The other part of the statement is clear. Q.E.D.

Now we fix L as before and a $\mathbb{Z}_p$-basis $x_1, \ldots, x_n$ of L. Before we proceed, we need a bit of notation:

Definition: For any finite R-module M, let

$$t(M) = |I \cdot M|^n.$$

We recall: $I \subset R$ is the augmentation ideal and n is fixed. The point of this is that we can now show:

Lemma 2.2. $\displaystyle\sum_{N \in Y(L)} t(E/N)^{-1} = 1.$

Proof: Let $X = \{(y_1, \dots, y_n) \in Rad(R)E^n : \alpha(y_i) = x_i,\ i = 1, \dots, n\}$. Clearly X is a principal homogeneous space under the additive group $IE^n = \ker(\alpha)^n$. The latter group is locally compact (even profinite) and carries a unique Haar measure μ which gives measure 1 to the whole group. Then X inherits this measure in an unambiguous fashion; we do not hesitate to call that measure μ as well. It is fairly easy to see that the subset X' of X defined by the extra condition that $y_1, \dots, y_n$ are R-independent satisfies $\mu(X') = 1$. In the sequel we will mostly calculate with X'; however, if it comes to measures, there is no difference between X and X'.

Now there is an obvious surjection $\nu : X' \to Y(L)$, which sends $(y_1, \dots, y_n)$ to the module $\langle y_1, \dots, y_n \rangle_R$. Let X'_N be the fiber of this map for $N \in Y(L)$. We claim:

$$\mu(X'_N) = \mu(IE^n \cap N^n). \qquad (*)$$

Indeed, pick $(y_1, \dots, y_n) \in X'_N$. For any other $(y'_1, \dots, y'_n) \in X'_N$, the difference $(y'_1 - y_1, \dots, y'_n - y_n)$ is obviously in N^n and in the kernel of $\alpha : E^n \to F^n$, hence in $IE^n \cap N^n$. The point is that we have a converse: for $(z_1, \dots, z_n) \in IE^n \cap N^n$, certainly $y'_i = y_i + z_i$ is in N, and we just have to show that the y'_i still generate N. For this it suffices to see that all z_i are in the radical of N, and this is true for the following reason: IE is the annihilator of $s = \sum_{\sigma \in \Delta} \sigma$ on E, so $IE \cap N$ is the annihilator of s on N; since N is R-free, this coincides with IN, and this is in the radical of N.

With the formula (*), we can finish the proof of Lemma 2.2: Since $\mu(IE^n) = 1$, we have $\mu(IE^n \cap N^n) = [IE : IE \cap N]^{-n} = |IE + N/N|^{-n} = t(E/N)^{-1}$. Formula (*) now gives, on summation over N:

$$\sum_{N \in Y(L)} t(E/N)^{-1} = \sum_{N \in Y(L)} \mu(IE^n \cap N^n) = \sum_{N \in Y(L)} \mu(X'_N) = \mu(X') = 1,$$

as was to be shown. Q.E.D.

We recall the statement of Theorem 1.2: For any finite $\mathbb{Z}_p$-module G, we want to prove

$$\sum_{M_\Delta \cong G} \mathsf{aut}_R^{-1}(M) = \mathsf{aut}^{-1}(G),$$

where the sum runs over *isomorphism classes of* finite R-modules M of projective dimension ≤ 1 satisfying $M_\Delta \cong G$. We can now prove this formula: Fix G and let n be the minimal number of generators of G. We consider all $\mathbb{Z}_p$-submodules $L \subset F = \mathbb{Z}_p^n$ such that $F/L \cong G$. Every finite R-module M is isomorphic to E/N for some R-submodule N of $E = R^n$, and if we let $L = \alpha(N)$ then $M_\Delta \cong G$ iff $F/L \cong G$. Moreover M has projective dimension at most one iff N is R-free, and L is in the radical of F iff N is in the radical of E. The rest will be counting arguments.

We define:

$$s = |\{\phi \in \mathsf{Hom}(F, G) : \phi \text{ is surjective}\}|$$

and (assuming $M_\Delta \cong G$)

$$s_M = |\{\psi \in \mathsf{Hom}_R(E, M) : \psi \text{ is surjective}\}|.$$

Then one checks easily that

$$s_M = t(M) \cdot s \quad (\text{recall } t(M) = |IM|^n).$$

On the other hand standard arguments show that:

$$|\{L \subset F : F/L \cong G\}| = s \cdot \mathsf{aut}^{-1}(G);$$
$$|\{N \subset E : E/N \cong M\}| = s_M \cdot \mathsf{aut}_R^{-1}(M).$$

Therefore we obtain (the condition $\mathrm{pd}(M) \leq 1$ is implicit):

$$\begin{aligned}
\sum_{M_\Delta \cong G} \mathsf{aut}_R^{-1}(M) &= s^{-1} \cdot \sum_{M_\Delta \cong G} s_M \cdot t(M)^{-1} \cdot \mathsf{aut}_R^{-1}(M) \\
&= s^{-1} \cdot \sum_{M_\Delta \cong G} |\{N \subset E : E/N \cong M\}| \cdot t(M)^{-1} \\
&= s^{-1} \cdot \sum_{M_\Delta \cong G} \sum_{E/N \cong M} t(M)^{-1} \\
&= s^{-1} \sum_{F/L \cong G} \sum_{N \in Y(L)} t(E/N)^{-1} \\
&= s^{-1} \sum_{F/L \cong G} 1 \quad \text{by Lemma 2.2} \\
&= s^{-1} \cdot |\{L \subset F : F/L \cong G\}| \\
&= \mathsf{aut}^{-1}(G).
\end{aligned}$$

Q.E.D.

3. Numerical observations for Δ of order p

As we said, our original motivation for this kind of heuristics was the observation that the minus class group of imaginary abelian extensions tends to be cohomologically trivial, and the existence of a link between the class group of imaginary quadratic fields $\mathbb{Q}(\sqrt{-r})$ (with r a prime congruent 3 mod 4 and congruent 1 mod p) and the minus class group of the abelian field K_r of degree $2p$ and conductor r. Thus, K_r is the subfield of degree $2p$ in the cyclotomic field $\mathbb{Q}(\zeta_r)$, and Δ is the subgroup of order p in the Galois group $\mathrm{Gal}(K_r/\mathbb{Q})$. It is quite reasonable to consider Δ and not the whole Galois group, since we are only considering the minus part of the class group, so the action of j (complex conjugation) does not carry any information.

In order to get a first idea how well the Galois equivariant heuristics of the introduction fit in with reality, we set $p = 3$ and looked at the totality of all primes r up to one million satisfying the above congruences. (The condition $r \equiv 3 \bmod 4$ ensures that K_r is imaginary; the condition $r \equiv 1 \bmod p$ ensures that K_r exists at all!)

The task was therefore to determine the 3-primary part $C(r)$ of the minus class group of K_r, and to examine its distribution. This was done in the spirit of Theorem 1.2, that is: we performed a preliminary classification according to $G(r) := C(r)_\Delta$, noting that this latter group is canonically isomorphic to the 3-primary part of the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-r})$. We shall report one some observations we made; we hope to be able to give more details in a forthcoming publication.

It is a direct consequence of Nakayama's lemma that $C(r)$ is zero iff $G(r)$ is zero. This (frequent) case is discarded to begin with. The first thing is now to distinguish two principal cases: (1) $G(r)$ cyclic but nonzero, and: (2) $G(r)$ non cyclic. According to the "ordinary" C-L heuristics, (1) should be much more frequent than (2), and this is just what happens: (1) happens for 7853 values, and (2) happens for just 251 values.

We deal with (1) first. Thus $G(r) = \mathbb{Z}/3^i\mathbb{Z}$ for some $i \geq 1$, and again by Nakayama, $C(r)$ is cyclic, i.e. isomorphic to R/I for some principal ideal I. (Recall $R = \mathbb{Z}_3[\Delta]$.) One has $\mathrm{Aut}(R/I) \cong (R/I)^*$ of cardinality $2 * 3^{j-1}$ where $|R/I| = 3^j$. Actually one easily shows that j has to be greater than i, and that for every $j > > i$ there exist exactly two principal ideals I of index 3^j in R with the property that $(R/I)_\Delta = \mathbb{Z}/3^i\mathbb{Z}$. Our heuristics would therefore imply that with i fixed, the frequency that $|C(r)| = 3^j$ is proportional to 3^{-j}. This agrees very well with our numerical evidence, assembled in the next table. The row index is i, the column index is j. Thus for example, there are 3472 cases of $G(r) = \mathbb{Z}/3\mathbb{Z}$ and $|C(r)| = 9$. The calculations were fairly easy, using Stickelberger elements.

	1	2	3	4	5	6	7	8	9	10	11	12
1	0	3472	1220	412	111	45	15	3	1	1	0	0
2	0	0	1098	370	132	43	15	4	2	0	0	1
3	0	0	0	408	124	50	11	6	3	0	0	0
4	0	0	0	0	164	44	12	10	1	1	1	0
5	0	0	0	0	0	45	12	8	3	0	1	0
6	0	0	0	0	0	0	1	1	1	0	0	1
7	0	0	0	0	0	0	0	0	0	0	0	0

For the sake of interest, we exhibit the two cyclic R-modules which belong to the couple $(i, j) = (1, 2)$. We call them $\mu_{4,9}$ and $\mu_{7,9}$; they are just $\mathbb{Z}/9\mathbb{Z}$ as abelian groups, and a fixed generator σ of Δ acts on them as multiplication by 4 respectively 7. Here we must highlight a ticklish point in our heuristics! We have no obvious means of canonically fixing a generator of Δ as r varies. This means that we have no reasonable way of distinguishing the two modules $\mu_{4,9}$ and $\mu_{7,9}$. They are not isomorphic, but when we change the generator of Δ (obviously there are two), these two modules get exchanged. Our strategy is therefore to always count two modules which are thus related simultaneously in our statistics; we pretend they are the same module, and we count it twice. This seems to work rather well, and we know of no other way out of this difficulty.

Next we turn to case (2). Here $G(r)$ needs exactly two generators, because the first occurrence where $G(r)$ needs three generators is $r = 3321607$ which is beyond

our search range. As we said, case (2) occurs for 251 values of r. (The smallest value is $r = 4027$.) To keep things simple, we will concentrate on one major subcase, that is, the 152 instances where

$$G(r) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Our task is here, in principle, to classify all cohomologically trivial modules M over $R = \mathbb{Z}_3\Delta$ such that $M_\Delta = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$; in particular, the modules M we are looking for need exactly two generators over R. It turned out early on that even this fairly modest task is not at all simple. There are, unsurprisingly, infinitely many modules M (up to isomorphism of course), and (perhaps a slight surprise) they tend to be indecomposable. The cardinal of M cannot be less than $81 = 3^4$. The table of our results will concentrate on modules M which occur "frequently", which is reasonable, given the fairly low size 152 of our sample. For the reader's convenience, let us present explicitly a few modules M. (The numbering goes according to frequency.)

We begin with decomposable modules. There are a priori three non-isomorphic ones which have the minimum cardinality 81: $M_9 = \mu_{4,9} \times \mu_{4,9}$; $M_2 = \mu_{4,9} \times \times \mu_{7,9}$; $M_9' = \mu_{7,9} \times \mu_{7,9}$. Again we have to be honest as to the unknown choice of generator of Δ. This means that we are unable to distinguish M_9 from M_9', so we omit M_9' and count M_9 twice. These are all decomposable modules of cardinality 81. There are exactly four isomorphism types of cohomologically trivial M which are indecomposable of cardinality 81. All of them have $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ as the underlying abelian group; a generator σ acts via multiplication by $E+3A$ with A a 2×2 matrix over $\mathbb{Z}/3\mathbb{Z}$, and the module is classified up to isomorphism by the characteristic polynomial of A:

$$\begin{aligned} M_1 &: (x-1)^2; \\ M_3 &: x^2 + x - 1; \\ M_3' &: x^2 - x - 1; \\ M_6 &: x^2 + 1. \end{aligned}$$

Again, M_3 and M_3' are undistinguishable, so we forget M_3' and count M_3 twice. There are two other modules we want to specify, both of order 3^5:

$$\begin{aligned} M_4 &= \mu_{4,9} \times R/3R; \\ M_5 &= \mu_{4,9} \times R/(\sigma^2 + \sigma + 4). \end{aligned}$$

Now we are ready to present a piece of our numerical results, namely the observed frequency of the 9 most common modules M, again under the standing hypothesis: $M_\Delta = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We compare with the predicted frequency which is, by Theorem 1.2 (note $\mathsf{aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) = 48$:)

$$48 \cdot \mathsf{aut}_R^{-1}(M).$$

It is not entirely trivial to calculate $\mathrm{aut}_R(M)$ of the involved modules, but it can be done. The reader might try to convince himself, as an example, that with $M_9 = \mu_{4,9} \times \mu_{4,9}$ we find $\mathrm{aut}_R(M_9) = 48 \cdot 81$. This is fairly large, and correspondingly M_9 should be "rare". This is the table of frequencies (rounded to 4 decimals):

Module	Expected	Observed
M_1	0.1975	0.2237
$M_2 = \mu_{4,9} \times \mu_{7,9}$	0.1481	0.1711
M_3	0.1481	0.1118
$M_4 = \mu_{4,9} \times R/3R$	0.0987	0.0987
$M_5 = \mu_{4,9} \times R/(\sigma^2 + \sigma + 4)$	0.0987	0.0658
M_6	0.0741	0.0855
$M_7 = \mu_{4,9} \times R/(\sigma^2 - 5\sigma - 2)$	0.0329	0.0329
$M_8 = \mu_{7,9} \times R/(\sigma^2 - 5\sigma - 2)$	0.0329	0.0132
$M_9 = \mu_{4,9} \times \mu_{4,9}$	0.0247	0.0329

The agreement is not everywhere very good, but the orders of magnitude are reflected very well. This continues if one prolongs the table, but we have given most of our results anyway (only 25 values out of 152 are not covered by the above table). One should try to obtain more data. Even for the classical C-L heuristics, agreement is good but not overwhelming in the range $r < 1$ million.

Unfortunately it will be fairly hard to obtain more data. Treating just one value of r involves, in principle, finding the class group of a sextic field with in general very high conductor. We used the system PARI which is excellently suited to calculations of this type, but even PARI's inbuilt function for calculating classgroups was on average too slow or did not terminate. We wrote an ad hoc algorithm in PARI which only calculates the minus class group. This took up to an hour on a Sun workstation, but the algorithm is still in its test phase, which means that many runs had to be aborted because some parameters were not chosen suitably. The total machine time consumed is thus much higher as the time consumed by the successful runs. It is hoped that the algorithm can be ameliorated and made more autonomous. Moreover the algorithm depends on heuristic assumptions, as most algorithms on class groups. The results however appear to be safe, since there is a quick method of calculating the minus class number (not the minus class group!), using Stickelberger elements. This check was done in every single case. Furthermore, an error would very likely have produced an R-module which is NOT cohomologically trivial, and this was not observed a single time either.

4. Divergence of the "big" Cohen-Lenstra sum

The convergence and the value of $S'(\mathbb{Z}_p[\Delta])$ for arbitrary p-groups Δ is not yet known in general. Things stand as follows: For cyclic Δ of order p^k there is a conjecture, see the Introduction; the conjecture is proved for $k = 1$, but again, for $k \geq 2$ not even convergence is known yet. On the other hand we can at least prove divergence for non-cyclic Δ. The main point is:

Proposition 4.1. *If Δ is the noncyclic group of order p^2 then $S'(\mathbb{Z}_p[\Delta]) = +\infty$.*

Proof: Fix a pair of generators σ, τ for Δ. We fix $n \geq 1$ for a moment. For every pair (A, B) of matrices in $(\mathbb{Z}/p)^{n\times n}$ we have a Δ-module $M_{A,B}$ which is just $(\mathbb{Z}/p^2)^n$ as an abelian group, and σ (resp. τ) act as multiplication by $E + pA$ and $E + pB$ respectively, where E is the $n \times n$ identity matrix. We are abusing notation here of course: pA has to be interpreted as p times a lift of A to $(\mathbb{Z}/p^2)^{n\times n}$, and similarly for pB. Then $E + pA$ runs precisely through all matrices in $GL(n, \mathbb{Z}/p^2)$ which are congruent to E modulo p. Note that $E + pA$ and $E + pB$ do have order 1 or p, and they do commute. The group $\Gamma = GL(n, \mathbb{Z}/p^2)$ acts on $X = (\mathbb{Z}/p)^{n\times n} \times (\mathbb{Z}/p)^{n\times n}$ via $C * (A, B) = (CAC^{-1}, CBC^{-1})$. The following two things are easily seen:

(a) Two modules $M_{A,B}$ and $M_{A',B'}$ are Δ-isomorphic iff the pairs (A, B) and (A', B') are Γ-conjugate.

(b) The stabilizer under Γ of any pair (A, B) is canonically isomorphic to the automorphism group of $M_{A,B}$ over $R = \mathbb{Z}_p[\Delta]$.

The Γ-orbits of X thus correspond to isomorphism classes of R-modules. Take the class equation which expresses $|X|$ as the sum of all terms $|\Gamma|/|Stab(A, B)|$, with the pairs (A, B) running modulo Γ-conjugacy, and divide it by $|\Gamma|^{-1}$. This yields

$$|X||\Gamma|^{-1} = \sum_M \mathsf{aut}_R^{-1}(M),$$

where the sum is over all modules $M = M_{A,B}$ modulo R-isomorphism. It is quite easy to evaluate the left hand side of this equation, and the result is $(1-q)^{-1} \cdots \cdots (1-q^n)^{-1}$, which is more than 1. Since we may take any $n \in \mathbb{N}$ whatsoever, the divergence of the sum $S'(R)$ now becomes quite evident. Q.E.D.

Corollary 4.2. *If Δ is a non cyclic p-group, then $S'(\mathbb{Z}_p[\Delta]) = +\infty$.*

Proof: The Frattini quotient $F(\Delta) = \Delta/([\Delta, \Delta]\Delta^p)$ of Δ is non-cyclic, and an elementary abelian p-group. We thus find a factor group $\bar{\Delta}$ of Δ which is noncyclic of order p^2. Whenever we have a quotient group $\bar{\Delta}$ of a group Δ, the sum $S'(\mathbb{Z}_p[\bar{\Delta}])$ can be seen as a sub-sum of $S'(\mathbb{Z}_p[\Delta])$, upon a moment's reflection. Thus Prop. 4.1 forces $S'(\mathbb{Z}_p[\Delta])$ to diverge as well. Q.E.D.

To conclude, we repeat: The only finite p-groups Δ which remain to be dealt with are the cyclic groups of order p^k with $k \geq 2$, and for them the problem remains open. For groups of order prime to p the corresponding problem is not too difficult: the big sum $S'(\mathbb{Z}_p[\Delta])$ and the small sum $S(\mathbb{Z}_p[\Delta])$ agree, and one has convergence; the details are left to the reader, the abelian case being particularly simple. It would be interesting to consider nonabelian groups whose order is divisible by p.

References

[1] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer Verlag 1995

[2] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, Number Theory Noordwijkerhout 1983, Springer Lecture Notes 1068, Springer Verlag 1984

[3] H. Cohen and J. Martinet, *Etude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39-76

[4] C. Greither, *The structure of some minus class groups, and Chinburg's third conjecture for abelian fields*, Math. Zeitschrift **229** (1998), 107-136

[5] P. Hall, *A partition formula connected with Abelian groups*, Comment. Math. Helv. **11** (1938-39), 126-129

[6] Electronic mail message from H. Lenstra, June 3rd, 1998

[7] L. Washington, *Some remarks on Cohen-Lenstra heuristics*, Math. Comp. **47** (1986), 741-747

Author's address: Cornelius Greither, Institut für theoretische Informatik und Mathematik, Fakultät für Informatik, Universität der Bundeswehr München, 85577 Neubiberg, F.R.Germany

E-mail: greither@informatik.unibw-muenchen.de

Received: June 23, 2000